ABSTRACT

A multi-step signing system and method uses multiple signing devices to affix a single signature which can be verified using a single public verification key. Each signing device posesses a share of the signature key and affixes a partial signature in response to authorization from a plurality of authorizing agents. In a serial embodiment, after a first partial signature has been affixed, a second signing device exponentiates the first partial signature. In a parallel embodiment, each signing device affixes a partial signature, and the plurality of partial signatures are multiplied together to form the final signature. Security of the system is enhanced by distributing capability to affix signatures among a plurality of signing devices and by distributing authority us affix a partial signature amond a plurality of authorizing agents.